NASA Public Key Infrastructure (PKI) Subscriber Agreement
(version 1.3.1 March 2002)

YOU MUST READ THIS NASA PKI SUBSCRIBER AGREEMENT BEFORE APPLYING FOR, ACCEPTING, OR USING A NASA PUBLIC KEY CERTIFICATE. IF YOU DO NOT AGREE TO THE TERMS OF THIS SUBSCRIBER AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE THE NASA PUBLIC KEY CERTIFICATE. BY SUBMITTING AN APPLICATION FOR A NASA PUBLIC KEY CERTIFICATE, YOU DEMONSTRATE YOUR KNOWLEDGE AND ACCEPTANCE OF THE TERMS OF THIS SUBSCRIBER AGREEMENT.

THIS NASA PKI SUBSCRIBER AGREEMENT will become effective on the date you submit your NASA Public Key Certificate application to your designated Registration Authority (RA) (the authority responsible for identifying and authenticating the identity of NASA Public Key Certificate applicants). By submitting a Certificate application you are requesting that the NASA Certification Authority (CA) (the authority that issues and manages NASA Public Key Certificates) issue a NASA Public Key Certificate to you and you are expressing your agreement to the terms of this Subscriber Agreement.

NASA Agency-Wide PKI Policy is governed by the X.509 Certificate Policy for NASA PKI. NASA Public Key Certificate Management Procedures (i.e., issuance, use and revocation of Certificates) are described in the NASA Certification Authority (CA) Certification Practice Statement (CPS). These and other relevant documents are published on the Internet at **http://nasaca.nasa.gov/docs.html**.

Within the NASA CA domain, each PKI user is both a Subscriber (an entity whose name appears as the subject of a public key certificate) and a Relying Party (an entity who uses a public key certificate to authenticate a digital signature or encrypt communications to the certificate subject).

IN THIS CA DOMAIN, PURSUANT TO THE NASA CA CPS, **EACH PKI USER, AS SUBSCRIBERS, MUST:**

- make true representation at all times to both the NASA CA and RA regarding information in his/her Certificate and other identification and authentication information;
- use Certificates exclusively for authorized NASA business, consistent with the X.509 Certificate Policy for NASA PKI and the NASA CA CPS;
- take reasonable precautions to protect his/her private keys and key tokens (if applicable) from loss, disclosure, modification, or unauthorized use;
- protect his/her private decryption keys and private signing keys through cryptographic mechanisms or storing them on a hardware token or a diskette. Within the NASA PKI, the NASA PKI software (i.e. Entrust) protects a subscriber's private keys through cryptographic mechanisms. The subscriber may further protect his/her private keys by storing them on a hardware token or diskette and, when not in use, removing the token or diskette from the computer and keeping the token or diskette on his/her person or stored in a secure, locked container or drawer;

- protect his/her user password, by not writing it down and not disclosing his/her password to others. If a subscriber is concerned about not remembering the password, he/she may store a written copy in secure, locked container or drawer;
- inform his/her local RA within 48 hours of a change to any information included in his/her Certificate or Certificate application request;
- inform his/her local RA within 8 hours of a suspected compromise of one/both of their private keys; and
- inform the RA when he/she no longer requires the Certificate, for reasons including job transfer, extended leave, resignation or termination of employment.

EACH PKI USER, AS RELYING PARTIES MUST:

- restrict use and reliance on Certificates issued by the NASA CA to appropriate uses for those Certificates, in accordance with the X.509 Certificate Policy for NASA PKI and in accordance with the NASA CA CPS;
- verify Certificates, including checking the Certificate Revocation Lists (CRLs) and Authority Revocation Lists (ARLs), taking into account any critical extensions (Within the NASA PKI, the NASA PKI software (i.e. Entrust) checks the CRLs and ARLs to confirm certificate validity.); and
- use and rely on Certificates only if a valid certificate chain is established between the Relying Party and the certificate subject.

CERTIFICATES MAY BE USED ONLY FOR PURPOSES RELATED TO NASA BUSINESS AND ARE SUITABLE FOR PROVIDING CONFIDENTIALITY, AUTHENTICATION, NON-REPUDIATION AND DATA INTEGRITY FOR NASA INFORMATION UP TO AND INCLUDING SENSITIVE BUT UNCLASSIFIED. CERTIFICATES ARE NOT TO BE USED FOR CLASSIFIED INFORMATION.

FAILURE TO ABIDE BY NASA CERTIFICATE POLICIES AND PRACTICES MAY CONSTITUTE GROUNDS FOR REVOCATION OF CERTIFICATE PRIVILEGES, AND MAY RESULT IN ADMINISTRATIVE ACTION AND/OR CRIMINAL PROSECUTION UNDER THE COMPUTER FRAUD AND ABUSE ACT (18 U.S.C § 1030(c)).

DISCLAIMER OF LIABILITY AND WARRANTIES

NASA DISCLAIMS ANY LIABILITY THAT MAY ARISE FROM USE OF ANY CERTIFICATE ISSUED BY A NASA CA, OR FROM THE DETERMINATION TO REVOKE A CERTIFICATE ISSUED BY A NASA CA. IN NO EVENT WILL NASA OR A NASA CA BE LIABLE FOR ANY DAMAGES, INCLUDING, BUT NOT LIMITED TO, DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, ARISING OUT OF OR RELATING TO ANY CERTIFICATE ISSUED OR REVOKED BY A NASA CA OR UNDER THE X.509 CERTIFICATE POLICY FOR NASA PKI AND THE NASA CA CPS.

NASA DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY

WARRANTY OF MERCHANTABILITY, ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTY OF ACCURACY OF INFORMATION CONTAINED WITHIN CERTIFICATES (EXCEPT THAT IT CAME FROM AN AUTHORIZED SOURCE).

NASA, AND THE NASA CA AND RAs ARE NOT LIABLE FOR ANY LOSS, INCLUDING LOSS:

- of CA or RA service due to war, natural disasters or other uncontrollable forces;
- incurred between the time a Certificate is revoked and the next scheduled issuance of a CRL;
- due to unauthorized use of Certificates issued by the NASA CA, and use of Certificates beyond the authorized uses defined by the X.509 Certificate Policy for NASA PKI and the NASA CA CPS;
- caused by fraudulent or negligent use of Certificates and/or CRLs and/or ARLs issued by the NASA CA; or
- due to disclosure of personal information contained within Certificates and/or CRLs and/or ARLs.

If any provision of this Agreement is declared by a court of competent jurisdiction to be invalid, illegal, or unenforceable, all other provisions shall remain in force.

NASA reserves the right to refuse to issue a NASA Public Key Certificate.

THIS AGREEMENT SHALL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH UNITED STATES FEDERAL LAW. NASA PUBLIC KEY CERTIFICATES ARE DEEMED GOVERNMENT SUPPLIED EQUIPMENT, AND AS SUCH, ALL PKI USERS, AS SUBSCRIBERS AND/OR RELYING PARTIES, ARE BOUND BY U.S. FEDERAL LAW GOVERNING THE USE OF GOVERNMENT PROVIDED EQUIPMENT.

AS A SUBSCRIBER AND/OR RELYING PARTY, YOU AGREE TO USE THE NASA PUBLIC KEY CERTIFICATE AND ANY RELATED NASA PKI SERVICES ONLY IN ACCORDANCE WITH THIS SUBSCRIBER AGREEMENT, THE NASA CA CPS AND THE X.509 CERTIFICATE POLICY FOR NASA PKI.